



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/047,275	01/15/2002	Erland Wittkottter		4501

826 7590 06/08/2004

ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000

EXAMINER

LY, ANH

ART UNIT	PAPER NUMBER
----------	--------------

2172

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/047,275

Applicant(s)

WITTKOTTER, ERLAND

Examiner

Anh Ly

Art Unit

2172

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 January 2002.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☐ Claim(s) _____ is/are rejected.
7) ☒ Claim(s) 1-20 is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is response to applicant's communication filed on 01/15/2002.
2. Claims 1-20 are pending in this application.

Specification

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Drawings

4. The drawings are objected to under 37 CFR 1.83(a) because they fail to show label for each box or the name of each as described in the specification. Any structural detail that is essential for a proper understanding of the disclosed invention should be shown in the drawing. MPEP § 608.02(d). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the claimed invention such as encryption symmetric key must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Applicant is required to submit a proposed drawing correction in reply to this Office action. However, formal correction of the noted defect may be deferred until after the examiner has considered the proposed drawing correction. Failure to timely submit the proposed drawing correction will result in the abandonment of the application.

Claim Rejections - 35 USC § 112

5. Claims 7, 8, 9, 12 and 13 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Since the claim 7, 8, 9, 12 and 13 are reciting the structure of claim 1 and the elements in these claims are differed from claim 1 in scope. Thus, it would not be a proper dependent claim, even though it placed further limitations on the remaining elements or added still other elements (See Infringement Test: MPEP 608.01(n)).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. US Patent No. 6,385,596 issued to Wiser et al. (hereinafter Wiser) in view of US Patent NO. 5,765,152 issued to Erickson.

With respect to claim 1, Wiser discloses a local computer unit which correspond to a local data file system for calling and for storing and for bi-directional data transferring of a volume data file by means of a computer unit and an user identification unit (client computer in the data processing over Internet with client/server architecture having stored local file system such as media data file and the passport is verified, see fig. 1, col. 5, lines 42-67 and col. 6, lines 1-28, col. 14, lines 6-18; col. 8, lines 43-67 and col. 9, lines 1-36), which is corresponding to the local computer unit, which enable an access on volume data files through the computer unit by an authorized user as a reaction on its positive identification only (media data file is delivered to the user or purchaser: col. 7, lines 4-15 and lines 48-45 and col. 8, lines 18-26), whereby the volume data file in the local data file system is stored in a encrypted to form, which is not usable for a user characterized in that a data transferring path of volume data files between the local computer unit and the local data file system (providing encryption from media player of the user personal information, from which the media player's public key and private keys to be encrypted the purchased media data: col. 4, lines 12-27 and col. 6, lines 28-46) comprise a corresponding key management unit as a part and functionality of the local computer unit, which generate and assign at least one user specific and volume data specific key file for each volume data file, the key management unit with a portion of the local data file system, which is connected to the

logically separated key database and for linking of a key file which is stored in the key database with a volume data file (the content of media data files including the encryption of media data files allowing a particular user to access stored in the transactions database: col. 9, lines 40-67) which is stored in a local data file system for, that is usable by an user (passport is stored in the local file system of client computer unit ; col. 14, lines 12-20).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach generating an electronic document and whereby the key database is provided locally in the data processing appliance and assigned to the local data file system, but logical or structural or physical separated from a drive - or mass storage unit.

However, Erickson teaches generating electronic media as well as electronic document (col. 14, lines 32-54) and physically separate data processing system from storage unit (col. 19, lines 40-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/ser architecture over the Internet network from which a

copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 2, Wiser teaches the encrypted form comprise the encryption by means of a symmetric key (security module is to use for encryption symmetric key: col. 21, lines 45-52; also see col. 4, lines 12-26, col. 7, lines 27-38 and col. 12, lines 16-18).

With respect to claim 3, Wiser discloses a data processing apparatus as discussed in claim 1. Wiser also teaches a content or meaning distorted interchanging, removing or attaching of file components (removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach the encrypted form referring of an electronic document as provided on a basis of a volume data file.

However, Erickson teaches generating electronic media as well as electronic document (col. 14, lines 32-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data

processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 4, Wiser teaches the local data file system is a database and the volume data file is a database register or database records of the database (the content of media data files including the encryption of media data files allowing a particular user to access stored in the transactions database: col. 9, lines 40-67).

With respect to claim 5, Wiser teaches the local data file system is a mass storage unit on a workplace with preferable a plurality of users (see fig. 1, item 126: a number of client computer systems or a number of users of the system: col. 5, lines 40-65).

With respect to claim 6, Wiser teaches the volume data files comprise digital text-, program-, image-, sound- and video files and combinations of these (media data files: col. 6, lines 47-67 and col. 7, lines 1-55).

With respect to claim 7, Wiser teaches identifying of an user who has access to a computer unit and who has access to a volume data files which is stored on a data file system that is assigned to a computer unit (client computer where the media data file to stored, in the data processing over Internet with client/server architecture having stored local file system such as media data file and the passport is verified, see fig. 1, col. 5, lines 42-67 and col. 6, lines 1-28, col. 14, lines 6-18; col. 8, lines 43-67 and col. 9, lines 1-36);

enabling an authorized access on user specific volume data file as a reaction on a positive identification (the media data file is delivered to the purchaser or an authorized user after verifying: col. 8, lines 1-10);

storing of the generated key file in a key storage unit (storing the key to be encrypted in a storage unit: col. 6, lines 28-46, col. 7, lines 38-45 and col. 8, lines 42-56);

reading of a volume data file and user specific key file as reaction on an access command of a user (reading the media data files for encryption via a file management module: col. 26, lines 58-67);

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach generating of a volume data file and user specific key file for an electronic document that is stored in the data file system and a subsequent linking of the electronic document with the key file for generating and storing of a volume data file, which is not usable for an user, and linking of the read-out key file with the volume data file that is given in a non-usable form for an user and that is read-out from the data file system and generating of an usable electronic document.

However, Erickson teaches generating electronic media as well as electronic document (col. 14, lines 32-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 8, Wiser teaches whereby the electronically stored original amount of data comprise a sequence of information components of a meta language in form of a written language, of a number system or of information component from data elements that are arranged in a predetermined, unitary format structure, in particular image-, sound- or program information and that are stored in a plurality of electronic addressable storage area (media data files including a variety of format file such video, sound or audio file image file text file and HTML. SGML or XML document or text files: col. 6, lines 48-67 and col. 7, lines 1-67);

interchanging or removing of an information component in the amount of data or attaching an information component at a predetermined position in the sequence of information components or exchange of an information components with a information component that is preferably not included in the original amount of data by a computer access on the respective storage area for generating of an amount of encrypted data (removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34);

generating an amount of key data with information on the interchanged, removed, attached or exchanged information component, which is designed in a manner, that a reconstruction of the original amount of data is permitted and (generating symmetric keys for encryption media data file keys; col. 7, lines 27-34);

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach storing of the amount of encrypted data and storing of the amount of key data in a separated, user specific key file within a common file system.

However, Erickson teaches physically separate data processing system from storage unit (col. 19, lines 40-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/ser architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 9, Wiser teaches whereby the electronically stored original amount of data comprise a sequence of information components of a meta language in form of a written language, of a number system or of information component from data

elements that are arranged in a predetermined, unitary format structure, in particular image-, sound- or program information and that are stored in a plurality of electronic addressable storage area, comprising the steps: Interchanging or removing of an information component in the amount of data or attaching an information component at a predetermined position in the sequence of information components or exchange of an information components with a information component that is preferably not included in the original amount of data by a computer access on the respective storage area for generating of an amount of encrypted data; generating an amount of key data with information on the interchanged, removed, attached or exchanged information component, which is designed in a manner, that a reconstruction of the original amount of data is permitted (media data files including a variety of format file such video, sound or audio file image file text file and HTML. SGML or XML document or text files: col. 6, lines 48-67 and col. 7, lines 1-67; removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34; and generating symmetric keys for encryption media data file keys; col. 7, lines 27-34).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach storing of the amount of encrypted data and storing of the amount of key data in a separated, user specific key file within a common file system.

However, Erickson teaches physically separate data processing system from storage unit (col. 19, lines 40-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 10, Wiser teaches the successive at least twofold encryption of the amount of key data whereby each is generated with the step of interchanging, removing, attaching or exchanging, whereby a first, hereby generated key data record is assigned to a first user and a second following generated key data record is assigned to a second user (col. 4, lines 12-67 and col. 5, lines 1-16; also see col. 9, lines 1-24; and removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

With respect to claim 11, Wiser teaches the successive at least twofold encryption of the amount of key data whereby each is generated with the step of interchanging, removing, attaching or exchanging, whereby a first, hereby generated key data record is assigned to a first user and a second following generated key data record is assigned to a second user (col. 4, lines 12-67 and col. 5, lines 1-16; also see

col. 9, lines 1-24; and removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

With respect to claim 12, Wiser teaches an encryption unit that is subordinated to the analyzing unit, which is designed for interchanging or removing of information components in the original amount of data or attaching of an information components at a predetermined position in the sequence of information components or exchanging of an information component with an information component that is preferably not contained in the original amount of data and creating an amount of key data with information about the interchanged, removed, attached or exchanged information components, which are designed in a manner, that a reconstruction of the original amount is permitted with key data, and a storage unit which is designed to store the amount of key data in a key data storage unit and a volume data storage unit, which is designed to store the amount of, encrypted data (multiple layers of encryption method: see abstract, media data files including a variety of format file such video, sound or audio file image file text file and HTML. SGML or XML document or text files: col. 6, lines 48-67 and col. 7, lines 1-67; removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34; and generating symmetric keys for encryption media data file keys; col. 7, lines 27-34).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does

not clearly teach an analyzing unit, which is designed to access on the original amount of data which are stored in a document storage unit and which is designed to electronically detect at least a sequence of information components of the original amount of data as a reaction on a predetermined or inspected format- or structural data of the original amount of data.

However, Erickson teaches authorizations to access the media or the media to the data processor and affixing minimum permission information to the data element, which specifies access restrictions to the data element (col. 7, lines 12-16 and col. 8, lines 58-67; and generating electronic media as well as electronic document: col. 14, lines 32-54)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 13, Wiser teaches an analyzing unit, which is designed to access on the original amount of data which are stored in a document storage unit and which is designed to electronically detect at least a sequence of information components of the original amount of data as a reaction on a predetermined or inspected format- or structural data of the original amount of data, an encryption unit

that is subordinated to the analyzing unit, which is designed for interchanging or removing of information components in the original amount of data or attaching of an information components at a predetermined position in the sequence of information components or exchanging of an information component with an information component that is preferably not contained in the original amount of data and creating an amount of key data with information about the interchanged, removed, attached or exchanged information components, which are designed in a manner, that a reconstruction of the original amount is permitted with key data, and a storage unit which is designed to store the amount of key data in a key data storage unit and a volume data storage unit, which is designed to store the amount of, encrypted data (multiple layers of encryption method: see abstract, media data files including a variety of format file such video, sound or audio file image file text file and HTML. SGML or XML document or text files: col. 6, lines 48-67 and col. 7, lines 1-67; removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34; and generating symmetric keys for encryption media data file keys; col. 7, lines 27-34).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does not clearly teach an analyzing unit, which is designed to access on the original amount of data which are stored in a document storage unit and which is designed to electronically detect at least a sequence of information components of the original

amount of data as a reaction on a predetermined or inspected format- or structural data of the original amount of data.

However, Erickson teaches authorizations to access the media or the media to the data processor and affixing minimum permission information to the data element, which specifies access restrictions to the data element (col. 7, lines 12-16 and col. 8, lines 58-67; and generating electronic media as well as electronic document: col. 14, lines 32-54)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

With respect to claim 14, Wiser discloses the encryption unit is assigned to an equivalence unit, which provide at least one information component in the original amount of data for at least one equivalent information component, that is electronically stored, whereby the equivalent information component is designed in a manner, that it match with the corresponding information component grammatically, metaphorically, syntactically or regarding its format (encryption: col. 3, lines 20-67 and col. 4, lines 12-27 and col. 6, lines 58-67 and col. 7, lines 1-12; and a plurality of syntax of format

language such as XML, SGML and HTML: col. 7, lines 17-26, col. 8, lines 57-67; also col. 11, lines 62-67 and col. 12, lines 1-10).

With respect to claim 15, Wiser teaches the encryption unit is designed to interconnect with a semantic rule-applying unit, so that the interchanging, removing, attaching or exchanging are arranged within the grammar, format, metaphoric or syntax and which are determined by the format- or structural data (encryption: col. 3, lines 20-67 and col. 4, lines 12-27 and col. 6, lines 58-67 and col. 7, lines 1-12; removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34; and multiple of formats: col. 7, lines 17-26, col. 8, lines 57-67; also col. 11, lines 62-67 and col. 12, lines 1-10).

With respect to claim 16, Wise teaches a random controller unit is assigned to the encryption unit, in which the interchanging, removing, attaching or exchanging of single information components or sequences of information component are controlled by the encryption unit randomly, in particular in a non reproducible manner (controlling a random number of encryption approach: col. 3, lines 64-67 and col. 4, lines 1-28; also see col. 7, lines 27-36; removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

With respect to claim 17, Wiser teaches an encryption parameter unit that is subordinated to the encryption unit, and is designed for storing or inserting predetermined parameter for the interchanging, removing, attaching or exchanging by

the encryption unit, in particular regarding a depth of encryption given by a number of interchanging, removing, attaching or exchanging operations (removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

With respect to claim 18, Wiser teaches a conversion unit that is subordinated to the encryption unit, and is designed for generating an electronic transferable volume data file for the amount of encrypted data and preferably an actively executable program- or script file for the amount of key data (encryption: col. 3, lines 20-67 and col. 4, lines 12-27 and col. 6, lines 58-67 and col. 7, lines 1-12).

With respect to claim 19, Wiser teaches the encryption unit is designed to generate a plurality of an amount of key data, which comprise at least one of the key data does not provide the reconstruction of the original amount of data while combining with the amount of encrypted data, but which lead to an amount of data after the combining, that is matched with the original amount of data in a syntactically, grammatically or format-related manner (encryption: col. 3, lines 20-67 and col. 4, lines 12-27).

With respect to claim 20, Wiser teaches an apparatus as discussed in claim 12. Also Wiser teaches removing the entries (removing the entries from the system: col. 7, lines 38-45 and col. 20, lines 18-34).

Wiser teaches a system for the secure distribution of music and related media over a telecommunications network, such as Internet under a client-server architecture, client computer having stored local file system, authoring tool to verify the content of data file, encrypting a media data file with a public key for the person's use. Wiser does

not clearly teach the analyzing unit is subordinated to the encryption unit and is designed in a manner that the amount of key data comprise information about the exchanging - or interchanging given by information component used to interchange, remove, attach or exchange.

However, Erickson teaches authorizations to access the media or the media to the data processor and affixing minimum permission information to the data element, which specifies access restrictions to the data element (col. 7, lines 12-16 and col. 8, lines 58-67; and generating electronic media as well as electronic document: col. 14, lines 32-54)

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of Wiser with the teachings of Erickson so as to have electronic media as well as electronic document in a secure and registered over the Internet network. The motivation being to have a data processing system under client/server architecture over the Internet network from which a copyright of an electronic media is protected and authenticated through digital signatures and encryption.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anh Ly whose telephone number is 703 306-4527 or via E-Mail: ANH.LY@USPTO.GOV. The examiner can normally be reached on 7:30 AM - 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene, can be reached on 703 305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703 746-7239.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks


Washington, D.C. 20231

or faxed to: Central Office (703) 872-9306 (Central Official Fax Number)

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308-6606 or 703 305-3900.

ANH LY 
MAY 24th, 2004


JEAN M. CORRIELUS
PRIMARY EXAMINER